STATE of ARIZONA

Arizona Department Of Administration	**Agency STANDARD**	**TITLE: Acceptable Use of ADOA Information Resources**
	A800-M3-S02 Rev 1.0	**Effective: July 20, 2007**

1. AUTHORITY

1.1. The authority for this Standard is based on Arizona Revised Statute 41-703 and the ADOA Policy A800 – Information Security Policy.

2. PURPOSE

2.1. The purpose of this Standard is to establish the responsibilities and restrictions to be complied with by all users of ADOA Information Resources.

3. SCOPE

3.1. This Standard applies to all ADOA employees, contractors and other entities using ADOA Information Resources.

For those ADOA employees participating in the ADOA Telework Program, this Standard shall be supplemented by an approved ADOA Telework Agreement. The ADOA Telework Program is subject to separate standards and policies.

3.2. The ADOA Director, in conjunction with the ADOA Information Security (AIS) Manager and the ADOA LAN Manager, is responsible for ensuring the effective implementation of ADOA Information Security Policy and Standards which reference the Statewide Information Technology Policies, Standards and Procedures (PSPs).

4. DEFINITIONS AND ABBREVIATIONS

4.1. **Acceptable Use –** the use of ADOA Information Resources that is authorized and meets ADOA policy and standards.

4.2. **Authorized Use –** the use of ADOA Information Resources that is:

A. performed according to designated duties stated in an employee's job description, as assigned by an employee's supervisor or as necessary to carry out the daily duties of the position; or

B. provided to a contractor to satisfy the services contracted by ADOA; or

C. required by another state agency or outside organization under an intergovernmental agreement or interagency service agreement (IGA/ISA).

4.3. **Authorized User –** an individual authorized to use ADOA Information Resources. This includes full or part-time ADOA employees, temporary employees, contractor personnel and non-employees providing services or

products to the agency and/or non-employees who are given access to ADOA Information Resources (e.g. other state agencies with intergovernmental agreements or interagency service agreements (ISA/ISAs), suppliers on contract or outside organizations).

4.4. **ADOA Information Resources -** any computing device, peripheral (e.g., printers, scanners, USB flash drives, CD/DVD), software, local and wide area networks (LAN and WAN), communications equipment (including Fax machines and telephones), communications software (including Internet, Intranet, and bulletin board access software), Virtual Private Network (VPN) or remote access capabilities and data distribution, electronic data or related consumable (e.g. paper, disk space, central processor time, network bandwidth), information and data owned or controlled by the ADOA.

4.5. **Personal Device or Software -** any computing device, peripheral (e.g., printers, scanners, mice, headphones, USB flash drives, switches, hubs, wireless devices, network devices, "jump" or "thumb" drives, external hard drives, PDAs, Ipods, MP3 players, etc.), software, communications equipment (including Fax machines and cellular telephones), communications software (including the Internet, Intranet, and bulletin board access software), Virtual Private Network (VPN) or remote access capabilities not owned or controlled by the ADOA.

5. STANDARD

5.1. ADOA Information Resources are intended to be used for state business purposes only. Limited use of these resources, such as Internet, email, workstation or printer (excluding information and data owned or controlled by the ADOA) for personal needs is permitted as long as such use is consistent with ADOA Policies and Standards and only when ALL of the following conditions are met:

A. No discernible additional cost or expense to the State is incurred.
B. There is no noticeable negative impact upon the employee's job performance.
C. There is no noticeable negative impact upon other State employees in the performance of their duties or provision of services.
D. It does not bring discredit or embarrassment to the State.
E. Does not violate this Standard.

5.2. Authorized users will not use ADOA Information Resources for illegal, inappropriate or obscene purposes.

5.3. Use of ADOA Information Resources for political or personal gain is prohibited.

5.4. **Authorized users will not connect any Personal Device or Software to the ADOA network via an Ethernet port, switch, router, wireless or any other connection without prior written approval from ADOA Information Security Manager and the authorized user's Division Assistant Director.** Any Personal Device or Software connected to the ADOA network is subject to inspection, seizure and/or destruction, unless specifically authorized in writing by the ADOA Information Security Manager and the Authorized User's Division Assistant Director. Exception is made for those with an approved ADOA Telework Agreement, who are using personal devices to connect from outside the ADOA network.

5.5. **Authorized users will not connect or install any Personal Device or Software to an ADOA desktop or laptop, without prior written approval from ADOA LAN Manager and the authorized user's Division Assistant Director.** Exception is made for those with an approved ADOA Telework Agreement, who are using personal devices to connect from outside the ADOA network. Any Personal Device or Software connected or installed to the ADOA network is subject to inspection, seizure and software destruction.

5.6. Authorized ADOA LAN users will not install, load or execute in memory any software application or program without first requesting such through ADOA LAN. ADOA LAN will be responsible for approval of all ADOA LAN and desktop software purchases, installation and tracking of those software licenses. The ADOA Chief Information Officer or their designee will approve all other software purchases.

5.7. ADOA may restrict the use of specific ADOA Information Resources through additional Standards. Divisions within ADOA may further restrict the use of ADOA Information Resources. ADOA Information Security will assume the responsibility for communicating any changes to these standards.

5.8. All use of ADOA Information Resources for electronic communication must represent ADOA in a manner that preserves the Agency's reputation and standards of professionalism. Any electronic communication that constitutes a significant representation of ADOA to the general public shall be approved by the appropriate Division Assistant Director**.** Consequently, any electronic communication discovered on an ADOA Website that is deemed inappropriate will be reported to ADOA Information Security and if necessary, the site will be disconnected until compliance can be achieved.

5.9. ADOA reserves the right to monitor all network traffic at any time, without prior notice or warning to the user. Anyone using ADOA Information Resources has **no expectation of privacy** in the use of these

tools or content. **Examples of improper use include but are not limited to**:

A. Illegal activities such as anti-trust or libel/slander.

B. Violation of copyrights (institutional or individual), other contracts or license agreements (e.g. downloading or copying data, software or music that is not authorized or licensed).

C. Knowingly or with willful disregard initiating activities that disrupt or degrade network or system performance, or wastefully using ADOA Information Resources.

D. Using ADOA Information Resources for fraudulent purposes.

E. Performing gambling activities or other illegal schemes (e.g. pyramid, chain letters, etc.).

F. Stealing or destroying ADOA Information Resources.

G. Misrepresenting another user's identification (forges or acts as), gaining or seeking to gain unauthorized access to another user's account/data.

H. Obtaining the passwords of other users or modifying or destroying another user's data.

I. Viewing, retrieving, saving or printing text or images of a sexual nature or containing sexual innuendo (e.g. accessing adult oriented sites or information via the Internet/Intranet or via email).

J. Invading systems, accounts or networks to obtain unauthorized access for the purpose of damaging (hacking). This includes unauthorized scans, probes, or system entries.

K. Connecting any unauthorized device to the ADOA Information Resources including the ADOA network.

L. Copying, transferring or emailing any ADOA data or information from ADOA Information Resources including the ADOA network, a desktop computer, wireless device, storage device or media without the explicit permission of the Authorized User's supervisor or manager.

M. Intentionally intercepting or modifying the content of a message or file originating from or belonging to another person without appropriate authorization.

N. Knowingly circulating destructive programs into ADOA Information Resources (e.g., worms, viruses, parasites, Trojan horses, malicious code, e-mail bombs, etc.).

O. Using ADOA Information Resources to conduct commercial or private business transactions, or support a commercial/private business, except as provided by the Arizona Administrative Code Title 2 (Administration), Chapter 11 (Department of Administration Public Buildings Maintenance), Article 3 (Solicitation) and Article 4 (Special Events).

P. Promoting fund-raising or advertising of non-State-sponsored organizations, except as provided by the Arizona

Administrative Code Title 2 (Administration), Chapter 11 (Department of Administration Public Buildings Maintenance), Article 3 (Solicitation) and Article 4 (Special Events) or Executive Order 2005-20 (Arizona State Employees Charitable Campaign).

Q. Generating or possessing material that is harassing, obscene, profane, intimidating or threatening, defamatory to a person or class of persons, or otherwise inappropriate or unlawful. This includes material that is intended only as a joke or for amusement purposes.

R. Disclosing protected or confidential ADOA Information Resources without proper authority.

S. Failing to comply with the instructions from appropriate ADOA management to discontinue activities that threaten the operation or integrity of ADOA Information Resources or those activities in violation of ADOA Policy and Standards.

5.10. Authorized users are responsible to protect and secure their ADOA Information Resources from unauthorized or improper use.

5.11. Users who suspect a misuse or attempted misuse of ADOA Information Resources or a violation of this Standard are obligated to immediately notify their supervisor and report the incident to the ADOA Help Desk.

6. STANDARD NON-COMPLIANCE

6.1. All authorized users of ADOA Information Resources are responsible for understanding and adhering to this Standard.

6.2. For non-compliance with this Standard, all ADOA employees shall be subject to Human Resource progressive discipline up to and including dismissal, with the exception that management may choose to take appropriate action commensurate with the seriousness of the offense. In addition, any non-compliance with this Standard that may constitute a violation of a State or Federal criminal statute may be referred to a law enforcement agency for appropriate action.

6.3. Contractors and other authorized users will be held to contractual agreements. In addition, any non-compliance with this Standard that may constitute a violation of a State or Federal criminal statute may be referred to a law enforcement agency for appropriate action.

7. REFERENCES

7.1. U.S. Code-Title 42-Subchapter XI-Part C-Sec 1320d-6-Wrongful disclosure of individually identifiable health information
7.2. Public Law 94-553, U.S. Copyright Law
7.3. ARS §13-2008. Taking identity of another person or entity; classification
7.4. ARS §13-2316, Computer tampering; venue; forfeiture; classification

7.5. ARS §38-448, State employees; access to internet pornography prohibited; cause for dismissal
7.6. ARS §39-101, Permanent public records; quality; storage; violation; classification
7.7. ARS §41-703, Duties of director
7.8. ARS §41-770, Causes for dismissal or discipline
7.9. ARS §41-1350, Definition of records
7.10. AAC R2-5-501, Standards of Conduct
7.11. Statewide Policy – P800, IT Security
7.12. ADOA Policy A800 – Information Security.

8. ATTACHMENTS

Acceptable Use of ADOA Information Resources Acknowledgement Form

ARIZONA DEPARTMENT OF ADMINISTRATION ACCEPTABLE USE OF ADOA INFORMATION RESOURCES ACKNOWLEDGMENT

I acknowledge that:

I have received, read, understand, and agree to abide by the ADOA Standard A800-M3-S02 - Acceptable Use of ADOA Information Resources.

_____ _____
Authorized User - Signature Supervisor - Signature

Date: _____

Authorized User Name (print): _____

Supervisor Name (print): _____

Agency or Division Name: _____